SCSUG

Smart Card Security Users Group

Defining Smart Card Security for the New Millennium

Gene Troy, NIST / NIAP

Chair, Smart Card Security Users Group

Common Criteria

SCSUG

Background

- The ultimate goal of smart card security is:
  - *proven robustness and correct functioning of every single card delivered to the card user*
- Chip security and Card life cycle security are the key links in this chain
- Becoming more important in view of --
  - multi-application cards
  - new applications demanding high security such as electronic purse
- Chip and card life cycle security are non-competitive issues

Common Criteria

SCSUG

Credit Cards & Smart Card Security

- Currently, Financial Payment Systems (i.e., *credit card brands*) individually do smart card evaluations -- Unstandardized, possibly conflicting
  - No global process to systematically compare vendors' security claims
- Vendor's products may be subject to conflicting requirements, repeated and expensive evaluations by different Users
- Vendors are the drivers in identifying product security requirements

Common Criteria

SCSUG

SCSUG's Approach

- **Smart Card Security Users Group (SCUSG):**
  - a global, financially oriented industry group including: American Express, Europay, JCB, MasterCard, Mondex, Visa
- **Coordinated by NIAP (US National Information Assurance Partnership)**
  - with the participation of other Governmental Bodies involved in the Common Criteria Project (Australia, Canada, France, Germany, UK)
- **Looking to the Common Criteria for IT Security Evaluation (ISO/IEC International Standard 15408) for security solutions**

Common Criteria

SCSUG

Common Criteria for IT Security Evaluation

- **ISO 15408 - Common Criteria for Information Technology Security Evaluation (the "CC")**
- **Currently endorsed by Australia, Canada, France, Germany, the Netherlands, New Zealand, United Kingdom, United States; others in Europe & Asia in process of joining**
- **A process for evaluating security of IT products**
- **Desperately needed for smart cards**

SCSUG

What IS the Common Criteria ??

What the Common Criteria is --

- **Common structure & language** for expressing product/system IT security requirements (Part 1)
- **Catalogs** of standardized IT security requirement components & packages (Parts 2 & 3)

How the CC is used --

- **Develop** Protection Profiles and Security Targets -- specific IT security requirements for products & systems -- *Consumers then use them for decisions*
- **Evaluate** products & systems against known & understood requirements → ***CONFIDENCE***

Common Criteria

SCSUG

Common Criteria Concepts (1)

The CC defines two types of IT Security Requirements:

Functional Requirements

- for defining security behavior of the IT product or system:

• implemented requirements become security functions

(what a product does)

Assurance Requirements

- for establishing confidence in Security Functions:

• correctness of implementation
• effectiveness in satisfying objectives

(is the product built well & does it meet its purpose)

Common Criteria

SCSUG

CC Concepts (2)
Evaluation Assurance Levels

(Basis for Mutual Recognition)

EAL	Name	OB/IT*
EAL1	Functionally Tested	
EAL2	Structurally Tested	C1 - E1
EAL3	Methodically Tested & Checked	C2 - E2
EAL4	Methodically Designed, Tested & Reviewed	E3
EAL5	Semiformally Designed & Tested	B2- E4
EAL6	Semiformally Verified Design & Tested	B3 - E5
EAL7	Formally Verified Design & Tested	A1 -E6

Common Criteria

*Rough Equivalences to: OB -- US "Orange Book", IT -- Europe's ITSEC

SCSUG

CC Concepts (3)
The PP & ST

- **Protection Profile -**
  - Statement of User's Security Requirements
  - Standard format, catalog of concepts & requirements
  - Implementation independent
- **Security Target**
  - Vendor creates to show how their product meets requirements
  - Implementation specific (= product)

Common Criteria

SCSUG

SCSUG's goals re CC

- Specify "Protection Profiles" for chip and operating system security based on the Common Criteria (ISO 15408) -- application independent
- Provide financial industry chip/card testing expertise to national schemes to aid rigorous industry-acceptable lab accreditation and testing standards.
- Use accredited Common Criteria Labs for the evaluation of vendor products against the defined profiles
- Agree a minimum set of product evaluation guidelines that produce reusable results

Common Criteria

SCSUG

SCSUG's CC-based Protection Profile

- SC-PP covers basic application-independent platform, including chip & operating software:
  - single or multiple applications supported
  - fixed or the new reconfigurable technologies
- Evolved from earlier work by each payment system, others
- NOTE: SC-PP's card security specs not limited to financial applications; threats/requirements generally applicable to "sensitive applications"

Common Criteria

Threats Addressed by SC-PP

- Physical attacks
  - e.g. probing, manipulation, modification
- Logical attacks
  - e.g. bad data, illegal program loading
- Access control
  - e.g. invalid access, impersonation
- Unanticipated Interactions
  - e.g. unallowed functions

SCSUG

More Threats Covered by SC-PP

- Cryptographic attacks
- Information monitoring
  - e.g. info “leakage”
- Miscellaneous
  - e.g. environmental stress, repetitive or linked attacks
- TOTAL THREATS: 23, all usage-oriented

Common Criteria

SCSUG

A Few of the 43 CC Functional Requirements in SC-PP

FAU_ARP.1	Security alarms
FAU_LST.1	Audit list generation
FCS_CKM.1	Cryptographic key generation
FCS_CKM.3	Cryptographic key access
FCS_COP.1	Cryptographic operation
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Information flow control
FDP_RIP.1	Residual information protection
FDP_UIT.1	Data exchange integrity

Common Criteria

SCSUG

A Few More SC-PP Security Functions

FIA_AFL.1	Authentication failure handling
FIA_UAU.7	Protected authentication feedback
FMT_MOF.1	Management of security functions behavior
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_RCV.3	Automated recovery without undue loss
FPT_RPL.1	Replay detection
FPT_RVM.1	Non-bypassability of the Security Policy
FTP_ITC.1	Inter-function trusted channel

Common Criteria

SCSUG

SC-PP Key Points

- Developed by a USER COMMUNITY (credit card brands / payment systems) to express their security requirements
- Intended as a communications tool with chip/card vendors and others
- Also intended as a basis for CC security evaluation to meet these users' needs
- Assurance level: EAL4+
  - Adds Design Modularity & stronger Vulnerability Analysis

Common Criteria

SCSUG

SC - Protection Profile Current Status

- Public draft was posted for 3-month comment period until January 31
- PP now completely revised to Version 2.0, ready for CC Lab evaluation, will be internationally registered when complete
- To become a *NIST Recommendation*

NOTE:

SC-PP also called out as security basis for GSA's Smart Access Common ID Card RFP (see Section J.7, Required Standards)

Common Criteria

Other SCSUG Activities

- Helping National Evaluation Schemes:
  - CC Evaluation Lab accreditation criteria (qualifications, equipment, procedures)
  - Evaluation methods to be used by labs
- Working with Semiconductor & Card vendors (e.g., SSVG)
  - to achieve agreement on common requirements & evaluation approaches

SCSUG

For More Information:

http://csrc.nist.gov/cc/sc/sclist.htm

- **American Express**
  Mark Merkow
  mark.merkow@aexp.com
- **Europay**
  Marijke de Soete
  mds@europay.com
- **JCB**
  Masanori Maeda
  maeda@cp.jcb.co.jp
- **MasterCard**
  Terry Stanley
  Terry_Stanley@mastercard. com
- **Mondex**
  Ken Warren
  ken.warren@mondex.com
- **NIAP**
  Gene Troy
  eugene.troy@nist.gov
- **Visa**
  Ken Ayer
  kayer@visa.com

Common Criteria

Copies of Slides available at:
http://csrc.nist.gov/cc -- smart cards